УДК 004.056.523
DOI: 10.31673/2409-7292.2023.030005

Дьячук О. С.

СТРАТЕГІЇ УПРАВЛІННЯ НАДІЙНИМИ ТА БЕЗПЕЧНИМИ ПАРОЛЯМИ: СУЧАСНІ ПІДХОДИ ТА РЕКОМЕНДАЦІЇ

У сучасному цифровому світі, де кількість онлайн-сервісів і ресурсів постійно зростає, забезпечення безпеки та надійності паролів є важливою задачею для користувачів. У даній статті пропонується огляд сучасних стратегій управління паролями та рекомендацій щодо створення надійних та безпечних парольних комбінацій.

Ключові слова: аутентифікація, пароль, доступ, аккаунт, ідентифікація, ключ, токен.

Вступ

У сучасному цифровому світі, де взаємодія з онлайн-сервісами, соціальними мережами та електронними ресурсами стала необхідністю, безпека персональних даних і конфіденційності стають особливо важливими. Одним із перших і найважливіших рівнів захисту є надійний та безпечний пароль. Проте, несвідоме використання слабких паролів або використання одного й того ж пароля для різних сервісів викладає нас ризику злому акаунтів, крадіжки особистої інформації та інших неприємних наслідків.

Мета цієї статті - оглянути сучасні стратегії управління надійними та безпечними паролями, а також надати читачам рекомендації та практичні поради щодо створення, зберігання та керування паролями. Ми розглянемо ключові аспекти, які допоможуть забезпечити високий рівень безпеки в онлайн-середовищі, враховуючи найновіші тенденції та вимоги.

Перший розділ присвячений аналізу сучасних стратегій управління паролями, включаючи силу пароля та важливість його компонентів. Ми розглянемо різні стратегії для створення унікальних паролів для різних сервісів і обговоримо переваги використання парольних менеджерів.

Другий розділ надасть читачам рекомендації та критерії для створення надійних та безпечних парольних комбінацій. Ми обговоримо довжину паролю, використання різних символів, а також розглянемо важливість уникання очевидних та прогнозованих паролів. Крім того, ми розглянемо необхідність частої зміни паролів та використання двофакторної аутентифікації, які є додатковими шарами захисту для забезпечення безпеки нашого аккаунту.

Третій розділ статті присвячений практичним порадам для безпечного зберігання та керування паролями. Ми обговоримо надійні методи зберігання паролів, включаючи використання парольних менеджерів та резервне копіювання паролів. Також ми поговоримо про захист від соціальної інженерії та фішингу, щоб запобігти злому паролів через маніпуляцію користувачем.

На завершення, в останньому розділі ми проведемо огляд інструментів та технологій, які допомагають автоматизувати управління паролями. Ми розглянемо нові тенденції, такі як біометрична аутентифікація, одноразові паролі та двофакторна аутентифікація з використанням мобільних пристроїв.

В цій статті ми намагатимемося зрозуміти, як налагодити баланс між надійністю та зручністю в управлінні паролями. Наша мета - надати читачам достатньо інформації та розуміння, щоб вони могли свідомо вибирати стратегії та інструменти, що найкраще відповідають їхнім потребам у безпеці.

1. Аналіз сучасних стратегій управління паролями

1.1 Сила пароля та ролі різних компонентів. Сила пароля залежить від його складності та унікальності. Сучасні стратегії управління паролями рекомендують використовувати комбінацію великих і малих літер, цифр та спеціальних символів. Кожен компонент додає до пароля додаткову складність і ускладнює завдання його злому (рис. 1) [1].

© Дьячук, О. С. (2023). Стратегії управління надійними та безпечними паролями: сучасні підходи та рекомендації. Сучасний захист інформації, 3(55), 38–44. https://doi.org/10.31673/2409-7292.2023.030005.

кількість символів	містить тільки цифри	малі літери	великі і малі літери	цифри, великі і малі літери	цифри, великі і малі літери, символи
4	Миттєво	Миттєво	Миттєво	Миттєво	Миттєво
5	Миттєво	Миттєво	Миттєво	Миттєво	Миттєво
6	Миттєво	Миттєво	Миттєво	1 сек	5 сек
7	Миттєво	Миттєво	25 сек	1 хвилина	6 хвилин
8	Миттєво	5 сек	22 хвилини	1 година	8 годин
9	Миттєво	2 хвилини	19 годин	3 дні	3 тижні
10	Миттєво	58 хвилин	1 місяць	7 місяців	5 років
11	2 сек	1 день	5 років	41 рік	400 років
12	25 сек	3 тижні	300 років	2л років	34к років
13	4 хвилини	1 рік	16к років	100к років	2млн років
14	41 хвилина	51 рік	800к років	9млн років	200млн років
15	6 годин	1к років	43млн років	600млн років	15млрд років
16	2 дні	34к років	2млрд років	37млрд років	1трлн років
17	4 тижні	800к років	100млрд років	2трлн років	93трлн років
18	9 місяців	23млн років	6трлн років	100трлн років	7квадрильйонів

Рис. 1. Залежність тривалості зламу від довжини пароля [8]

1.2 Стратегії створення унікальних паролів для різних сервісів. Застосування одного й того ж пароля для різних сервісів є серйозним ризиком. Якщо один пароль стає відомим зловмиснику, то всі наші аккаунти стають уразливими. Сучасні стратегії рекомендують створювати унікальний пароль для кожного сервісу. Для полегшення цього процесу можна використовувати парольні менеджери, які зберігають паролі і автоматично заповнюють їх на веб-сайтах [2].

1.3 Використання парольних менеджерів та їх переваги. Парольні менеджери - це програми або сервіси, які допомагають зберігати, керувати та генерувати паролі. Вони зберігають паролі в зашифрованому вигляді і заповнюють їх автоматично на веб-сайтах. Переваги використання парольних менеджерів включають [3]:

зручне зберігання та автоматичне заповнення паролів;

генерація випадкових, складних паролів;

можливість синхронізації паролів між різними пристроями;

високий рівень безпеки завдяки шифруванню даних.

Аналіз сучасних стратегій управління паролями демонструє, що використання ск ладних та унікальних паролів разом з використанням парольних менеджерів є ключовими компонентами безпечного управління паролями. Ці стратегії допомагають зменшити ризик злому паролів і зберегти конфіденційні дані.

1.4 Аналіз множини факторів аутентифікації. Одним з ефективних способів забезпечити безпеку паролів є використання множини факторів аутентифікації. Крім звичайного введення пароля, цей підхід включає додаткові шари захисту, такі як біометричні дані (відбиток пальця, розпізнавання обличчя) або використання одноразових кодів, які надсилаються на мобільний пристрій користувача. Аналіз різних факторів аутентифікації дозволяє з'ясувати, які з них є найбільш надійними та зручними для використання [4].

1.5 Значення освіти та свідомого підходу до управління паролями. Освіта користувачів про наслідки слабких паролів та важливість безпеки є невід'ємною частиною сучасних

© Дьячук, О. С. (2023). Стратегії управління надійними та безпечними паролями: сучасні підходи та рекомендації. Сучасний захист інформації, 3(55), 38–44. https://doi.org/10.31673/2409-7292.2023.030005.

стратегій управління паролями. Чим більше користувачі розуміють ризики і приймають свідомі рішення щодо своєї безпеки, тим менші ймовірність використання слабких паролів або недостатніх стратегій управління паролями [5].

Аналіз сучасних стратегій управління паролями показує, що надійне та безпечне управління паролями є критичним фактором для захисту особистих даних та уникнення кіберзагроз. Використання складних та унікальних паролів, парольних менеджерів, множини факторів аутентифікації та освіта користувачів про безпеку паролів створюють надійне забезпечення наших цифрових активів.

Однак, необхідно враховувати, що загрози в галузі кібербезпеки постійно розвиваються, і зловмисники шукають нові способи злому паролів. Тому важливо постійно оновлювати свої стратегії управління паролями, слідкувати за новими рекомендаціями та використовувати передові технології для захисту своїх аккаунтів.

У цій статті ми розглянули основні аспекти сучасних стратегій управління паролями. Ми дослідили силу пароля та роль різних компонентів, стратегії створення унікальних паролів для різних сервісів, переваги використання парольних менеджерів, аналіз множини факторів аутентифікації та важливість освіти користувачів у цій сфері.

Надіємося, що ця стаття надала вам цінну інформацію та практичні рекомендації, як управляти надійними та безпечними паролями. Пам'ятайте, що безпека паролів є одним із основних кроків для забезпечення захисту ваших особистих даних і цифрових активів.

2. Рекомендації щодо створення надійних та безпечних паролів

2.1 Довжина пароля. Одним з основних аспектів надійного пароля є його довжина. Рекомендується створювати паролі, які складаються з принаймні 12 символів. Чим довший пароль, тим складніше його зламати методами перебору.

2.2 Складність пароля. Пароль повинен бути складним і неочевидним для зловмисників. Включайте в нього великі і малі літери, цифри та спеціальні символи. Уникайте використання очевидних комбінацій, таких як "password" або "123456", а також особисто зв'язаних даних, таких як дата народження або ім'я.

2.3 Унікальність пароля. Кожен сервіс або акаунт повинен мати унікальний пароль. Використання одного й того ж пароля для різних сервісів є ризикованим, оскільки в разі порушення безпеки одного з них всі інші стають уразливими. Використовуйте парольні менеджери для зберігання та автоматичного заповнення унікальних паролів для кожного облікового запису.

2.4 Часта зміна паролів. Раніше рекомендувалося часто змінювати паролі, але останні дослідження показують, що ця практика може бути неефективною. Замість того, щоб змінювати паролі за регулярним графіком, краще зосередитись на створенні сильних та унікальних паролів, а також вживати заходів безпеки, таких як використання двофакторної аутентифікації.

2.5 Використання фрази або вигаданих слів. Один зі способів створення надійного пароля - це використання фрази або вигаданих слів зі спеціальними символами та цифрами. Наприклад, ви можете використовувати фразу, таку як "ЯЛюблюМатематику!", і перетворити її на пароль, замінюючи деякі символи на цифри та спеціальні символи: "ЯЛюблюМ4т3м@т!ку!".

2.6 Захист від соціальної інженерії. Соціальна інженерія є поширеною технікою атаки, де зловмисники намагаються отримати доступ до паролів шляхом маніпуляцій з людьми. Уникайте надання паролів чи особистих даних невідомим особам через телефон, електронну пошту або соціальні мережі. Будьте обережні при відповідях на запити, які можуть виглядати підозріло.

2.7 Використання двофакторної аутентифікації. Двофакторна аутентифікація (2FA) є ефективним методом забезпечення додаткового шару безпеки для вашого облікового запису.

© Дьячук, О. С. (2023). Стратегії управління надійними та безпечними паролями: сучасні підходи та рекомендації. Сучасний захист інформації, 3(55), 38–44. https://doi.org/10.31673/2409-7292.2023.030005.

При використанні 2FA потрібно буде ввести не тільки пароль, але й додатковий код, який буде надісланий на ваш мобільний пристрій або згенерований спеціальним додатком.

2.8 Регулярна перевірка і оновлення програм та пристроїв. Безпека пароля також залежить від загальної безпеки вашої системи. Важливо регулярно оновлювати програми та операційні системи на вашому комп'ютері або мобільному пристрої. Це допоможе запобігти використанню вразливостей, які можуть бути використані зловмисниками для отримання доступу до вашого пароля.

Враховуючи ці рекомендації, ви зможете створити та управляти надійними та безпечними паролями для своїх різних облікових записів. Пам'ятайте, що безпечні паролі є важливою складовою безпеки вашої онлайн присутності. Незабезпечені паролі можуть призвести до несанкціонованого доступу до особистої інформації, втрати фінансових коштів або навіть крадіжки особистої ідентичності.

Запам'ятайте, що хороший пароль має бути довгим, складним та унікальним. Використовуйте парольні менеджери для зберігання та керування вашими паролями, а також активуйте двофакторну аутентифікацію, де це можливо. Регулярно перевіряйте і оновлюйте ваші паролі, а також використовуйте останні версії програм та операційних систем.

У другому розділі ми розглянули ключові рекомендації щодо створення надійних та безпечних паролів. Застосування цих рекомендацій допоможе вам забезпечити високий рівень безпеки для ваших облікових записів та уникнути потенційних загроз.

У наступному розділі ми розглянемо стратегії використання парольних менеджерів та множини факторів аутентифікації для подальшого покращення безпеки паролів.

3. Практичні поради для безпечного зберігання та керування паролями

3.1 Використання парольних менеджерів. Одним з найефективніших способів керування паролями є використання парольних менеджерів. Ці програми дозволяють зберігати всі ваші паролі в зашифрованій формі під одним головним паролем. Вони також можуть генерувати випадкові, складні паролі для вас та автоматично заповнювати поля входу на веб-сайтах. При виборі парольного менеджера, переконайтеся, що він має хорошу репутацію та надійні механізми захисту даних.

3.2 Силка на основний пароль (Master Password). Оскільки головний пароль дозволяє отримати доступ до всіх інших паролів у парольному менеджері, важливо вибрати сильний та унікальний головний пароль. Уникайте використання очевидних фраз або особисто зв'язаних даних. Крім того, не рекомендується зберігати головний пароль у текстовому файлі або на листку паперу. Запам'ятайте його або використовуйте надійну методику збереження, наприклад, використовуючи фразу, яку тільки ви знаєте.

3.3 Автоматичне оновлення паролів. Парольні менеджери можуть пропонувати функцію автоматичного оновлення паролів. Це може бути корисно в разі виявлення потенційних порушень безпеки на веб-сайтах або сервісах, з якими пов'язані ваші облікові записи. Використовуючи цю функцію, ви можете оновити свої паролі одним натисканням кнопки, що забезпечує постійну безпеку ваших облікових записів.

3.4 Безпечне синхронізування та резервне копіювання. Якщо ви використовуєте парольний менеджер на кількох пристроях, важливо забезпечити безпечну синхронізацію між ними. Використовуйте рішення, які використовують сильне шифрування та забезпечують захист вашої інформації під час передачі між пристроями.

Крім того, рекомендується регулярно створювати резервні копії вашого парольного менеджера та зберігати їх у безпечному місці. Це дозволить вам відновити ваші паролі в разі втрати або пошкодження пристрою.

3.5 Множина факторів аутентифікації. Додатковим шаром безпеки для вашого облікового запису є використання множини факторів аутентифікації (MFA). Ви можете налаштувати MFA для вашого електронного поштового акаунту, соціальних мереж, онлайн-банкінгу та інших сервісів. Це означає, що після введення правильного пароля вам також буде

© Дьячук, О. С. (2023). Стратегії управління надійними та безпечними паролями: сучасні підходи та рекомендації. Сучасний захист інформації, 3(55), 38–44. https://doi.org/10.31673/2409-7292.2023.030005.

потрібно підтвердити свою ідентичність за допомогою додаткового фактора, такого як SMS-код, мобільний додаток аутентифікації або фізичний пристрій, такий як ключ безпеки.

3.6 Безпека фізичного доступу. Не забувайте про безпеку фізичного доступу до ваших пристроїв. Впевніться, що ваш комп'ютер, смартфон або планшет захищені паролем або відбитком пальця. Уникайте залишати незаблокований пристрій без нагляду, особливо в публічних місцях.

3.7 Регулярне оновлення паролів. Незважаючи на використання парольного менеджера та сильних паролів, рекомендується регулярно оновлювати ваші паролі. Плануйте періодичні зміни паролів для вашого безпеки. Рекомендується змінювати паролі щонайменше раз на 3-6 місяців. При цьому не використовуйте один і той же пароль для різних облікових записів. Застосовуйте унікальні паролі для кожного сервісу.

3.8 Безпека під час передачі паролів. Коли ви вводите або передаєте свої паролі, піклуйтеся про безпеку цього процесу. Використовуйте захищене підключення (HTTPS) при вході на веб-сайти та уникайте вводити паролі на публічних або ненадійних комп'ютерах. Уникайте також надсилання паролів через електронну пошту або повідомлення, оскільки ці канали можуть бути піддаються атакам або перехопленню даних.

4. Огляд інструментів та технологій для автоматизації управління паролями

4.1 Парольні менеджери. Парольні менеджери - це програми, що дозволяють зберігати, керувати та автоматично заповнювати паролі для різних облікових записів. Вони забезпечують безпечне зберігання паролів у зашифрованому вигляді, використовуючи майстер-пароль або інші методи аутентифікації. Деякі популярні парольні менеджери включають LastPass, 1Password (рис. 2), Dashlane і KeePass. Вони пропонують додаткові функції, такі як генерація складних паролів, синхронізація між пристроями і автоматичне оновлення паролів.

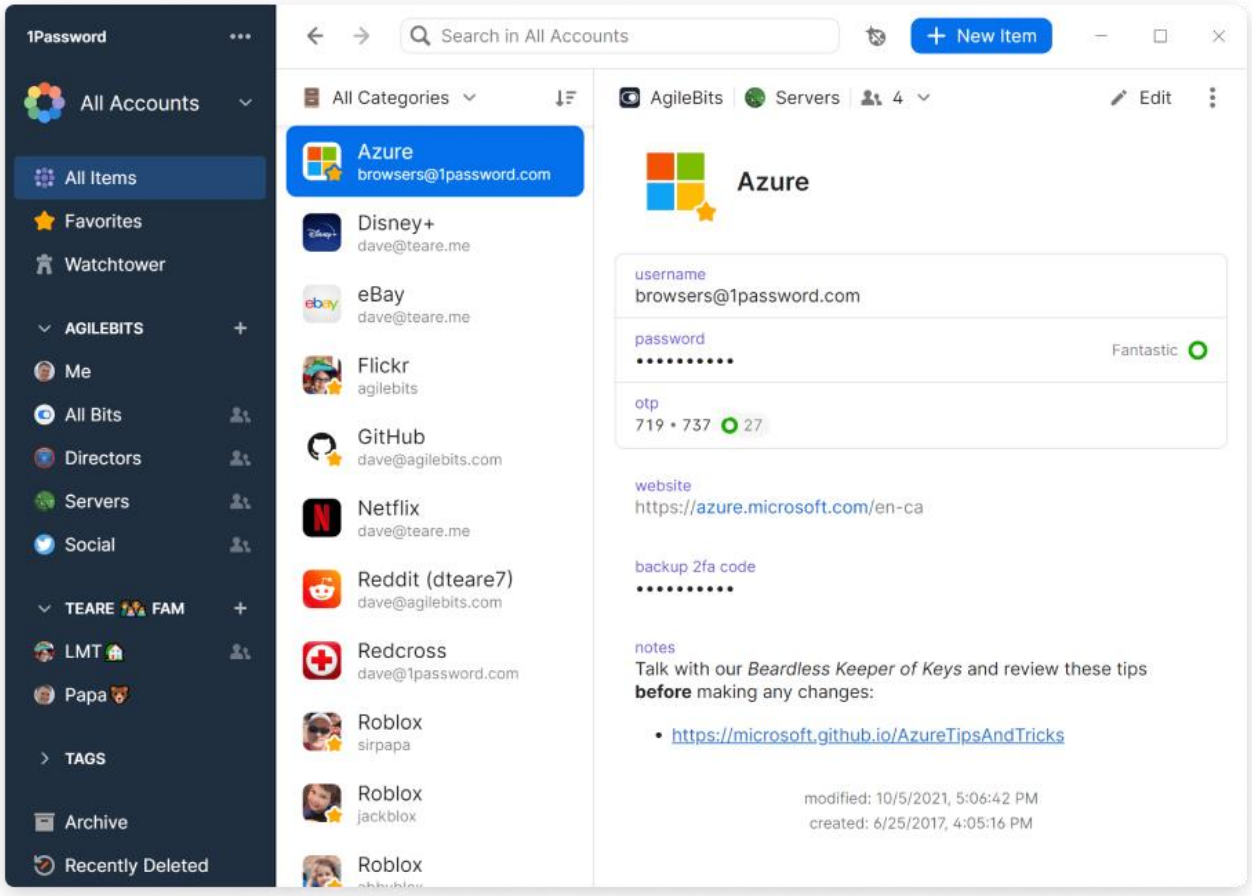

Рис. 2. Приклад інтерфейсу менеджера паролів 1Password [6]

© Дьячук, О. С. (2023). Стратегії управління надійними та безпечними паролями: сучасні підходи та рекомендації. Сучасний захист інформації, 3(55), 38–44. https://doi.org/10.31673/2409-7292.2023.030005.

4.2 Множини факторів аутентифікації. Множина факторів аутентифікації (MFA) додає додатковий шар безпеки до процесу входу в систему. Вона вимагає введення двох або більше факторів ідентифікації, таких як пароль, фізичний ключ, SMS-код або біометричні дані. Це робить вторгнення в обліковий запис важким навіть при викраденні пароля. Популярні методи MFA включають використання аутентифікаторів, які генерують одноразові паролі, а також фізичних пристроїв, таких як ключі безпеки або смарт-карти.

4.3 Біометрична аутентифікація. Біометрична аутентифікація використовує фізичні характеристики користувача, такі як відбиток пальця, розпізнавання обличчя або сканування раковини, для підтвердження ідентичності. Це забезпечує високий рівень безпеки, оскільки біометричні дані унікальні для кожного користувача і складно підробити. Біометрична аутентифікація використовується в смартфонах, планшетах, ноутбуках та інших пристроях. Вона забезпечує зручний спосіб входу в систему, оскільки не потрібно запам'ятовувати або вводити паролі. Проте варто пам'ятати, що біометричні дані можуть бути скомпрометовані, тому важливо обирати пристрої та сервіси з надійною системою зберігання цих даних.

4.4 Одноразові паролі. Одноразові паролі (OTP) - це унікальні паролі, які можуть бути використані тільки один раз і мають обмежений строк дії. Вони генеруються за допомогою спеціальних алгоритмів або відправляються на мобільний пристрій користувача через SMS або додаток. OTP можуть бути використані як додатковий фактор аутентифікації або як заміна сталих паролів. Вони забезпечують високий рівень безпеки, оскільки пароль стає недійсним після використання або закінчення терміну дії.

4.5 Фізичні ключі безпеки. Фізичні ключі безпеки - це фізичні пристрої, які забезпечують безпеку автентифікації шляхом використання криптографічних ключів. Вони можуть бути у формі USB-ключів, смарт-карт або NFC-токенів (рис. 3). Фізичні ключі безпеки вимагають фізичного доступу та фізичного взаємодії з пристроєм для підтвердження ідентичності. Вони забезпечують високий рівень безпеки, оскільки крадіжка або викрадення ключа є надзвичайно складним.

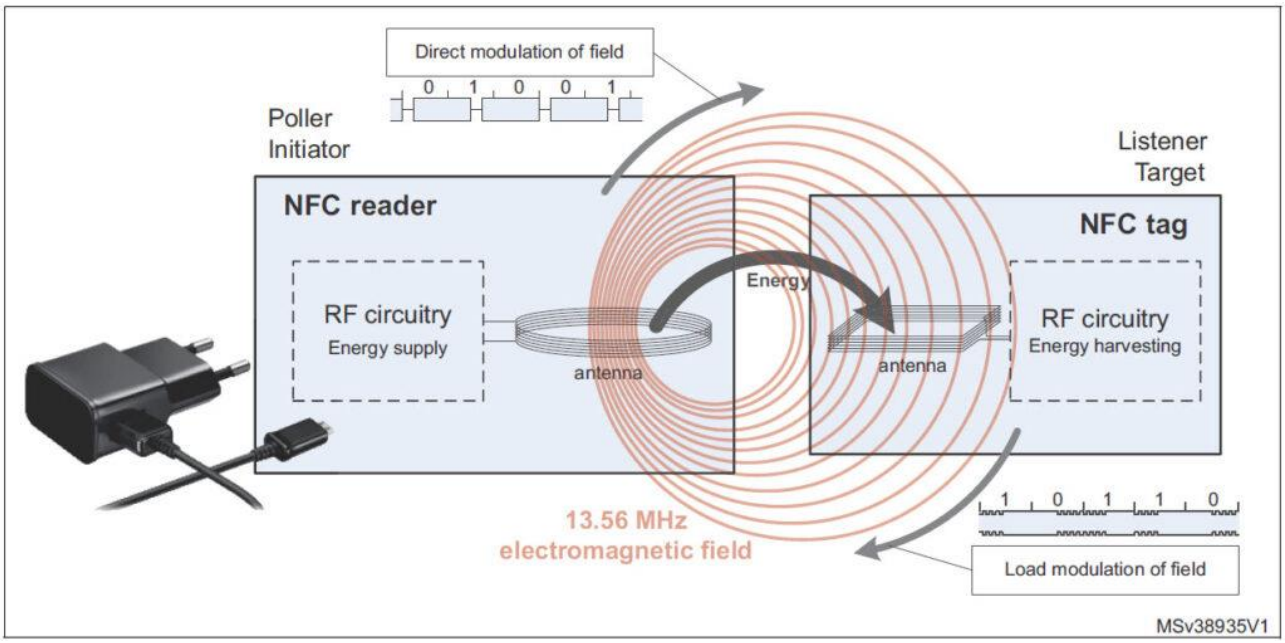

Рис. 3. Схема роботи NFC-токена [7]

Висновки

Існує багато інструментів та технологій, які допомагають автоматизувати управління паролями і забезпечують високий рівень безпеки. Парольні менеджери є потужними інструментами, що дозволяють зберігати та керувати паролями для різних облікових записів.

© Дьячук, О. С. (2023). Стратегії управління надійними та безпечними паролями: сучасні підходи та рекомендації. Сучасний захист інформації, 3(55), 38–44. https://doi.org/10.31673/2409-7292.2023.030005.

Вони забезпечують зручне і безпечне зберігання паролів і автоматичне заповнення форм входу.

Множина факторів аутентифікації (MFA) використовує два або більше фактори ідентифікації для забезпечення додаткового рівня безпеки. Вона може включати в себе аутентифікатори, фізичні ключі безпеки та біометричні дані, які унікальні для кожного користувача.

Біометрична аутентифікація використовує фізичні характеристики користувача для підтвердження ідентичності. Вона забезпечує зручний та безпечний спосіб входу в систему, оскільки не потрібно запам'ятовувати паролі.

Одноразові паролі (OTP) і фізичні ключі безпеки також забезпечують високий рівень безпеки. OTP можуть бути використані як додатковий фактор аутентифікації, а фізичні ключі безпеки вимагають фізичного доступу для підтвердження ідентичності.

Кожен з цих інструментів та технологій має свої переваги і недоліки, і важливо вибрати той, що найкраще підходить для вашої конкретної потреби. Рекомендацією є використовувати комбінацію цих методів для максимальної безпеки.

Управління надійними та безпечними паролями є важливим аспектом забезпечення безпеки вашої особистої інформації та онлайн активності. Використовуючи рекомендації цього розділу, ви можете створити, зберігати та керувати вашими паролями з високим рівнем безпеки. Пам'ятайте про важливість використання парольних менеджерів, множини факторів аутентифікації та безпеку фізичного доступу до ваших пристроїв. Практикуючи ці принципи, ви забезпечите захист вашої онлайн присутності та особистої інформації.

Перелік посилань

1. Chiradeep Basu Mallick. Top 10 Penetration Testing Tools in 2022. Gaw, Shirley & Felten, Edward. (2006). Password management strategies for online accounts. 44-55. 10.1145/1143120.1143127.

2. Alodhyani, F., Theodorakopoulos, G., & Reinecke, P. (2020). Password Managers - It's All about Trust and Transparency. Future Internet, 12, 189.

3. Karole, Ambarish & Saxena, Nitesh & Christin, Nicolas. (2010). A Comparative Usability Evaluation of Traditional Password Managers. 233-251. 10.1007/978-3-642-24209-0_16.

4. Yıldırım, M., Mackie, I. Encouraging users to improve password security and memorability. Int. J. Inf. Secur. 18, 741–759 (2019). https://doi.org/10.1007/s10207-019-00429-y

5. AlFayyadh, B., Thorsheim, P., Jøsang, A., & Klevjer, H. (2012). Improving Usability of Password Management with Standardized Password Policies.

6. https://1password.com/downloads/windows/

7. Scott Thornton. NFC Tag Basics: How to use for programming automation. May 31, 2018. https://www.microcontrollertips.com/programming-automation-using-nfc-tags-faq/

8. Вадим Георгієнко. Скільки часу потрібно для зламу вашого паролю? https://www.prostir.ua/?blogs=skilky-chasu-potribno-dlya-zlamu-vashoho-parolyu.

Надійшла: 03.08.2023 Рецензент: д.т.н., професор Савченко В.А.

© Дьячук, О. С. (2023). Стратегії управління надійними та безпечними паролями: сучасні підходи та рекомендації. Сучасний захист інформації, 3(55), 38–44. https://doi.org/10.31673/2409-7292.2023.030005.